ABSTRACT

In one embodiment, a method for certifying an attestation key comprises generating a remote attestation key pair within a platform and producing a certificate. The certificate includes a public attestation key to attest that a private attestation key, corresponding to the public attestation key, is stored in hardware-protected memory.